

Лабораторная работа №1

Математические основы защиты информации и
информационной безопасности (02.04.02)

Левкович К. А.

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

Информация

- Левкович Константин Анатольевич
- студент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223450@rudn.ru



Вводная часть

- Изучение базовых принципов шифрования
- Важность знания основ шифрования для работы в сфере информационных технологий

- Шифры простой замены
 - Шифр Цезаря
 - Шифр Атбаш

- Ознакомиться с шифрами простой замены
- Программно реализовать шифры

- Национальный Открытый Университет “ИНТУИТ”
- Язык программирования Python

Выполнение лабораторной работы

Шифр Цезаря

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

```
alphabet_ceaser = "abcdefghijklmnopqrstuvwxyz"

def shifr_ceaser(input_text, k=3):
    global alphabet_ceaser
    output_text = ""
    for char in input_text:
        if char in alphabet_ceaser:
            output_text += alphabet_ceaser[(alphabet_ceaser.index(char)+k) % 26]
        else:
            output_text += char
    return output_text
```

Шифр Атбаш

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я
я ю э ы ь щ щ ч ч х ф у т е р п о н м л к й и з ж е д г в б а

```
def shifr_atbash(input_text, alphabet="abcdefghijklmnopqrstuvwxyz"):
    output_text = ""
    len_alp = len(alphabet)
    for char in input_text:
        if char in alphabet:
            output_text += alphabet[len_alp - alphabet.index(char)-1]
        else:
            output_text += char
    return output_text
```

```
24  if __name__ == "__main__":
25      input_text = "my name is - kostya"
26      print(shifr_ceaser(input_text,3))
27
28      alphabet_atbash = "abcdefghijklmnopqrstuvwxyz"
29      atbash_text = "az"
30      print(shifr_atbash(atbash_text))
```

ПРОБЛЕМЫ

ВЫХОДНЫЕ ДАННЫЕ

КОНСОЛЬ ОТЛАДКИ

ТЕРМИНАЛ

ЛУ

```
PS D:\Dev\MatInfBez\lab1> & C:/Users/avgor/AppData/Local/M
pb qdph lv - nrwbd
za
```

Результаты

- Ознакомился с шифрами простой замены: шифр Цезаря, шифр Атбаш

- Ознакомился с шифрами простой замены: шифр Цезаря, шифр Атбаш
- Программно реализовал шифры с помощью языка программирования Python